SYSTEM AND METHODS FOR ADAPTIVE BEHAVIOR BASED ACCESS CONTROL

ABSTRACT OF THE DISCLOSURE

Typical conventional content based database security scheme mechanisms employ a predefined criteria for identifying access attempts to sensitive or prohibited data. An operator, identifies the criteria indicative of prohibited data, and the conventional content based approach scans or “sniffs” the transmissions for data items matching the predefined criteria. In many environments, however, database usage tends to follow repeated patterns of legitimate usage. Such usage patterns, if tracked, are deterministic of normal, allowable data access attempts. Similarly, deviant data access attempts may be suspect. Recording and tracking patterns of database usage allows learning of an expected baseline of normal DB activity, or application behavior. Identifying baseline divergent access attempts as deviant, unallowed behavior, allows automatic learning and implementation of behavior based access control. In this manner, data access attempts not matching previous behavior patterns are disallowed.